REMARKS

The Examiner rejected Claims 1, 6-7, 13, 18-19, 25 and 30-31 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,278,901 to Shieh et al. (Shieh), in view of U.S. Patent No. 5,440,723 to Arnold et al. (Arnold). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove.

Specifically, the Examiner has relied on the following excerpt from Shieh to meet applicant's claimed measuring "one or more measurement parameters indicative of non virus specific activity of said computer apparatus over a respective measurement period" and comparing "said one or more measurement parameters with respective predetermined threshold levels."

> "The indirect-write pattern of virus propagation, namely Iw(virus, o_i), may appear individually or simultaneously and can be detected by the model of the present invention using the following conditions: (1) |v.. set(out, Iw/Iw*, virus)|>threshold and a large portion of elements are executable files; (2) |C.. set(out, Iw/Iw*, virus)|>threshold; (3) |v.. set(in, cb/cb*/Icb/Icb*, virus)|>threshold; (4) |C.. set(in, cb/cb*/Icb/Icb*, virus)|>threshold; (5) v.. set(out, Id/Id*, virus)|>threshold; (6) |C.. set(out, Id/Id*, virus)|>threshold. The used here are parameters defining limits to determine abnormal process behavior. If the occurrences of a pattern exceeds the threshold, an abnormality occurs." (col. 17, lines 17-30)

Such excerpt along with the remaining Shieh reference, however, fails to disclose, teach or even suggest applicant's claimed "one or more measurement parameters indicative of non virus specific activity of said computer apparatus over a respective measurement period" (emphasis added).

Specifically, each of the conditions mentioned in the above excerpt are a function of a "virus," and thus do not meet applicant's claimed specific measurement parameters that are indicative of non virus specific activity. Only applicant teaches and claims such a threshold-based virus detection method that is based on non virus specific activity, as specifically claimed.

Further, the conditions outlined in the Shieh reference make absolutely no mention of any time dependence. Thus, Shieh fails to meet applicant's claimed measurement of the related

parameters over a respective measurement period. This feature is clearly absent in Shieh, as is evidenced by the foregoing excerpt.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim limitations

Nevertheless, in order further distinguish the art of record and in the interest of expediting the prosecution of the present application, applicant has incorporated the subject matter of Claims 2 et al. into each of the independent claims.

The Examiner rejected Claims 2-5, 14-17, and 26-29 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,278,901 to Shieh et al. (Shieh), in view of U.S. Patent No. 5,440,723 to Arnold et al. (Arnold), and further in view of U.S. Patent No. 5,832,208 to Chen et al. (Chen). Applicant respectfully disagrees with such rejection.

Specifically, now claimed in each of the independent claims is the former subject matter of Claim 2, namely "wherein one of said measurement parameters is how many e-mail messages are sent having an identical message title." It appears that the Examiner has simply dismissed applicant's claim limitations of Claims 2-5, 14-17, and 26-29 as being obvious in view of the teachings of Chen.

It is noted that the Examiner has not pointed to any particular excerpt from Chen to meet applicant's claimed features including the "identical message title"-based measurement parameter. Moreover, such feature, as well as the other measurement parameter features, are deemed beneficial (and not obvious), since they provide for improved ways of detecting a virus outbreak based on non virus specific activity.

It thus appears that the Examiner is relying on Official Notice to address applicant's claimed features of Claims 2-5, 14-17, and 26-29. In response, applicant again points out the remarks above that clearly show the manner in which such claims further distinguish applicant's claimed invention from the proposed combination. Applicant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

> "If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

Applicant further notes that there are numerous deficiencies with respect to the dependent claims. Just by way of example, the Examiner relies on the following excerpt from Shieh to make a prior art showing of applicant's claimed "wherein one of said measurement parameters is e-mail throughput within said computer system." See Claim 6 et al.

> "In particular, the present invention helps define patterns of object privilege and data flows that characterize operational security problems in otherwise secure systems. These problems include those caused by (1) the unintended use of foreign programs, (2) the unintended use of foreign input data, (3) the imprudent choice of default privileges, and (4) the use of weak protection mechanisms. However, as is the case with any model that requires explicit definition of intrusion patterns, the present invention detects only intrusions that can be anticipated prior to their occurrence. In general, pattern-oriented intrusion detection is intended to complement, not replace, statistical approaches for intrusion detection." (col. 4, lines 45-59)

Such excerpt, however, merely mentions data flows, but simply does not even suggest "e-mail throughput," let alone such feature in combination with the remaining features. Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all the claim

limitations. Thus, a notice of allowance or a specific prior art showing of such feature, in combination with the remaining claim elements is respectfully requested.

Still yet, the Examiner has simply dismissed the following limitations as being well-known: "wherein each e-mail processed has an associated size value and e-mail throughput is measured in a form dependent upon a number of e-mails multiplied by a total of size values for said e-mails." See Claim 7 et al. It again appears that the Examiner is relying on Official Notice, and a specific prior art showing (in the specific context of the remaining claim limitations) is respectfully requested.

The Examiner rejected Claims 8-9, 20-21, and 32-33 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,278,901 to Shieh et al. (Shieh), in view of U.S. Patent No. 5,440,723 to Arnold et al. (Arnold), and further in view of U.S. Patent No. 5,124,943 to Lubarsky (Lubarsky). The Examiner has further rejected Claims 10-12, 22-24, and 34-36 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,278,901 to Shieh et al. (Shieh), in view of U.S. Patent No. 5,440,723 to Arnold et al. (Arnold), and further in view of U.S. Patent No. 5,956,481 to Walsh et al. (Walsh). After careful review of such rejections, applicant notes that it appears that the Examiner has not taken into consideration the full weight of applicant's claims, and a specific prior art showing of each of the claim limitations is respectfully requested.

A notice of allowance is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P154).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100